EC-2000-007
IV-D-033

South Coast
Air Quality Management District
AQMD
21865 E. Copley Drive, Diamond Bar, CA 91765-4182
(909) 396-2000 • http://www.aqmd.gov

Office of the Executive Officer
Barry R. Wallerstein, D.Env.
909.396.2100, fax 909.396.3340

November 27, 2001

Enforcement and Compliance Docket and Information Center
Mail Code 2201A
1200 Pennsylvania Avenue NW
Washington, DC 20460

Attention: Docket Number EC-2000-007

Subject: Comments on Establishment of Electronic Reporting: Electronic Records; Proposed Rule

Ladies and Gentlemen:

The South Coast Air Quality Management District (SCAQMD) staff is pleased to offer the following preliminary comments on the United States Environmental Protection Agency (US EPA) Proposed Rule on Electronic Reporting: Electronic Records published in the Federal Register on August 31, 2001 (Volume 66, Number 170). However, the SCAQMD staff needs additional time to analyze the proposal and make meaningful recommendations that will improve the final rule. Therefore we are requesting the US EPA to extend the public comment period by 90 days. In addition, several thousand regulated businesses and entities may be impacted eventually by this rule. It is our understanding that no public hearings have been held in the West by US EPA, to date. The SCAQMD would like to encourage you to hold a public workshop on this important proposal in Southern California before finalizing the proposed rule.

We are very supportive of EPA efforts to allow the use of electronic reporting in local environmental programs. However, Part 3 Subpart D Sec. 3.2000 paragraphs (e), (f) and (g) of the proposed rule contains very prescriptive language, which exclude the use of the standards based electronic document receiving system we envision. The system we envision utilizes commercially available off-the-shelf e-mail software and Public Key Infrastructure (PKI) to provide authentication, data integrity and

nonrepudiation. This system could meet all other performance requirements in the proposed rule. Therefore, we request that Part 3 Subpart D Sec. 3.2000 paragraphs (e), (f) and (g) be eliminated in their entirety from the proposed rule to allow for flexibility in this area of rapidly changing technology.

However, if the elimination of these paragraphs is unacceptable to US EPA, then we strongly suggest that these paragraphs be revised as indicated in the form of strikeouts and underlines in the attached copy of Part 3 Subpart D containing these paragraphs.

The SCAQMD staff would also request clarification on the implementation of this rule by the US EPA, Region IX, with respect to the local administration of our air program. It is important for us to ensure that we can take advantage of the benefits of electronic reporting, while ensuring the enforceability of our compliance program and compliance with State Implementation Plan requirements under the Clean Air Act. These are important issues that we hope to resolve jointly with US EPA, Region IX, and the California Air Resources Board.

Please direct questions or comments to Peter Mieras at (909-396-3459 or pmieras@aqmd.gov) or Chris Marlia at (909-396-3148 or cmarlia@aqmd.gov).

Thank you for this opportunity to comment on the proposed rule.

Sincerely,

Barry R. Wallerstein, D.Env.
Executive Officer

BRW/drw
Enclosures

(9) Archive electronic records and documents in an electronic form which preserves the context, meta data, and audit trail, and, if required, must ensure that:
  (i) Complete records can be transferred to a new system;
  (ii) Related meta data can be transferred to a new system;
  (iii) Functionality necessary for use of records can be reproduced in new system; and

(b) Computer systems (including hardware and software), controls, and attendant documentation maintained under this Part must be readily available for, and subject to, agency inspection.

(c) Where electronic records bear electronic signatures that meet the requirements in paragraphs (a)(4) and (a)(5) of this section, EPA will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by federal or federally authorized State, tribal or local government environmental regulations, unless specifically excepted by regulations(s) effective on or after [date of promulgation of this regulation].

Sec. 3.200 [Reserved]

Subpart D—Electronic Reporting and Recordkeeping Under EPA- Approved State Programs

Sec. 3.1000 How are authorized State, tribal or local environmental programs modified to allow electronic reporting?

(a) State, tribes, or local environmental programs that wish to receive electronic reports or documents in satisfaction of requirements under such programs must revise or modify the EPA-approved State, tribal, or local environmental program to ensure that it meets the requirements of this part. The State, tribe, or local government must use existing State, tribal, or local environmental program procedures in making these program revisions or modifications.

(b) In order for EPA to approve a program revision under paragraph (a) of this section the State, tribe, or local government must demonstrate that electronic reporting under this program will:
  (1) Use an acceptable electronic document receiving system as specified under Sec. 3.2000;
  (2) Require that any electronic report or document must bear valid electronic signatures, as provided in Sec. 3.10 (c), (d) and (e), to the same extent that the paper submission for which it substitutes would bear handwritten signatures under the State, tribal, or local environmental program.

Sec. 3.2000 What are the criteria for acceptable electronic document receiving systems?

An electronic document receiving system that is acceptable for purposes of receiving electronic reports or documents submitted under provisions of an authorized State, tribal or local environmental program must meet all of the following requirements:

(a) General system-security. An acceptable electronic document receiving system must:
  (1) Have strong and effective protections against unauthorized access to the system;
  (2) Have strong and effective protections against the unauthorized use of any electronic signature on electronic documents submitted or received;
  (3) Provide for the detection of unauthorized access or attempted access to the system and unauthorized use or attempted use of any electronic signature on electronic documents submitted or received;
  (4) Prevent the modification of an electronic document once an electronic signature has been affixed;
  (5) Ensure that the electronic documents and other files necessary to meet the requirements under paragraphs (f) and (g) of this section are protected from modification or deletion;
  (6) Ensure that the system clock is accurate and protected from tampering or other compromise; and

(7) Have strong and effective protections against any other foreseeable corruption or compromise of the system.

(b) Validity of data. An acceptable electronic document receiving system must generate data sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that:
(1) The electronic document was not altered in transmission or at any time after receipt; and
(2) The electronic document was submitted knowingly and not by accident; and
(3) In the case of documents requiring the signature of an individual, that the document was actually submitted by the authorized signature holder and not some other person.

(c) Electronic signature method. By virtue of its presence as a part of an electronic document submitted or received, an electronic signature must uniquely identify the particular individual who has used it to sign an electronic document or otherwise certify to the truth or accuracy of the document contents; therefore, an acceptable electronic document receiving system must only validate electronic signatures created with a method that:
(1) Meets the registration requirements of paragraph (d) of this section;
(2) Meets the signature/certification requirements of paragraph (e) of this section;
(3) Prevents an electronic signature from being excised, modified, or copied for re-use without detection once it has been affixed to an electronic document by the authorized individual;
(4) Provides protection against the use of a specific electronic signature by unauthorized individuals;
(5) Ensures that it is impossible to modify an electronic document without detection once the electronic signature has been affixed.

(d) Submitter registration process. An acceptable electronic document receiving system must require that anyone who submits an electronic document to the system first register with the agency to which the document is to be submitted. The registration process must establish the identities of both the registrant, who is the prospective submitter, and any entity that the registrant is authorized to represent, and must establish that the registrant is authorized to submit the document in question for the entity being represented. In addition, where the documents to be received will require signature, the registration process must:
(1) Establish the registrant's identity, and the registrant's relation to any entity for which the registrant will submit electronic documents, with evidence that can be verified by information sources that are independent of the registrant and the entity or entities in question and that would be sufficient to identify the registrant as the signature holder for purposes of supporting litigation consistent with paragraph (b) of this section;
(2) Establish and document a unique correlation between the registrant and the code or device that will constitute or create the electronic signature of the registrant as a submitter;
(3) Require that the registrant sign on paper, or in such other manner or medium as the Administrator in his or her discretion may determine as appropriate for a category of electronic reports, an electronic signature agreement specifying at a minimum that the registrant agrees to:
(i) Protect the electronic signature from unauthorized use, and follow any procedures specified by the agency for this purpose;
(ii) Be held as legally bound, obligated, or responsible by use of the assigned electronic signature as by hand-written signature;

(iii) Where the signature method is based on a secret code or key, maintain the confidentiality of each component of the electronic signature;

(iv) In any case, never to delegate the use of the electronic signature, or in any other way intentionally provide access to its use, to any other individual for any reason; and

(v) Report to the entity specified in the electronic signature agreement, within twenty-four hours of discovery, any evidence of the loss, theft, or other compromise of any component of an electronic signature;

(4) Provide for the automatic and immediate revocation of an electronic signature in the event of:

(i) Any actual or apparent violation of the electronic signature agreement;

(ii) Any evidence that the signature has been compromised, whether or not this is reported by the registrant to whom the signature was issued; or

(iii) Notification from an entity that the registrant is no longer authorized by the entity to submit electronic documents on its behalf;

(5) Require that the registrant periodically renew his or her electronic signature agreement, under terms that the Administrator determines provide adequate assurance that the criteria of paragraphs (a) and (b) of this section are met, taking into account both applicable contractual provisions and industry standards for renewal or re-issuance of signature codes or devices.

(e) Electronic signature/certification scenario. An acceptable electronic document receiving system that may be used to accept electronic documents bearing an electronic signature must:

(1) Not allow an electronic signature to be affixed to the electronic document until:

(i) The signatory has been provided an opportunity to review all of the data to be transmitted in an on-screen visual format that clearly associates the descriptions or labeling of the information being requested with the signatory's response and which format is identical or nearly identical to the visual format in which a corresponding paper document would be submitted; and

(ii) The signatory takes affirmative action to affix his or her electronic signature~~A certification statement that is identical to that which would be required for a paper submission of the document appears on-screen in an easily-read format immediately above a prompt to affix the certifying signature, together with a prominently displayed warning that by affixing the signature the signatory is agreeing that he or she is the authorized signature holder -- referred to by name -- has protected the security of the signature as required by the electronic signature agreement signed under paragraph (d)(3) of this section and is otherwise using the signature in compliance with the electronic signature agreement~~;

(2) ~~Automatically r~~Respond to the receipt of an electronic document with transmission of an electronic acknowledgment in a timely fashion that:

(i) States that the signed electronic document has been received, clearly identifies the electronic document received, indicates how the signatory may view ~~and download~~ a copy of the electronic document received ~~from a read-only source~~, and states the date and time of receipt; and

~~(ii) Is sent to an address whose access is controlled by password, codes or other mechanisms that are different than the controls used to gain access to the system used to sign/certify and send the electronic document;~~

(3) Automatically creates an electronic ~~"copy of record"~~archive of the submitted report ~~that includes all the warnings, instructions and certification statements presented to the signatory during the signature/certification scenario as described under paragraph (e)(1) of this section, and~~ that:

(i) Can be viewed by the signatory, in its entirety, on-screen in a human-readable format that clearly and accurately associates all of the information provided by the signatory with the descriptions or labeling of the information that was requested;

(ii) Includes the date and time of receipt stated in the electronic acknowledgment required by paragraph (e)(2) of this section;

~~(iii) Has an agency electronic signature affixed that satisfies the requirements for electronic signature method under paragraphs (c) (3), (c) (4), and (c) (5) of this section;~~

(iv) Is archived by the system in compliance with requirements paragraph (g) of this section;

(v) Is made available to the submitter for viewing ~~and down-loading~~ in a timely fashion; and

(vi) Is protected from a unauthorized access.

(f) Transaction Record. An acceptable electronic document receiving system must create a transaction record for each received electronic document that includes:

~~(1) The precise routing of the electronic report from the submitter's computer to the electronic document receiving system;~~

(2) The precise date and time (based on the system clock) of:

(i) Initial receipt of the electronic document;

(ii) Sending of electronic acknowledgment under paragraph (e)(2) of this section;

(iii) ~~Copy of record~~Archive created under paragraph (e)(3) of this section;

(3) ~~Copy of record~~Archive as specified under paragraph (e)(3) of this section.

(g) System archives. An acceptable electronic document receiving system must:

(1) Maintain:

(i) The transaction records specified under paragraph (f) of this section, and

~~(ii) Records of the system on-screen interface displayed to a user under paragraph (e) of this section that can be correlated to the submission of any particular report (including instructions, prompts, warnings, data formats and labels, as well as the sequencing and functioning of these elements);~~

(2) Maintain the records specified under paragraph (g)(1) of this section for at least the same length of time as would be required for a paper document that corresponds to the received electronic document, and in a way that:

(i) Can be demonstrated to have preserved them in their entirety without alteration since the time of their creation; and

(ii) Provides access to these records in a timely manner that meets the needs of their authorized users.

Sec. 3.3000 How are authorized State, tribal or local environmental programs modified to allow electronic recordkeeping?

(a) State, tribes, or local environmental programs that wish to allow the maintenance of electronic records or documents in satisfaction of requirements under such programs must revise or modify the EPA-approved State, tribal, or local environmental program to ensure that it meets the requirements of this part. The State, tribe, or local government must use existing State, tribal or local environmental program procedures in making these program revisions or modifications.

(b) In order for EPA to approve a program revision under paragraph (a) of this section the State, tribe, or local government must demonstrate that records maintained electronically under this program will satisfy the requirements under Sec. 3.100 of this part.

Sec. 3.4000 [Reserved]

(iii) Where the signature method is based on a secret code or key, maintain the confidentiality of each component of the electronic signature;

(iv) In any case, never to delegate the use of the electronic signature, or in any other way intentionally provide access to its use, to any other individual for any reason; and

(v) Report to the entity specified in the electronic signature agreement, within twenty-four hours of discovery, any evidence of the loss, theft, or other compromise of any component of an electronic signature;

(4) Provide for the automatic and immediate revocation of an electronic signature in the event of:

(i) Any actual or apparent violation of the electronic signature agreement;

(ii) Any evidence that the signature has been compromised, whether or not this is reported by the registrant to whom the signature was issued; or

(iii) Notification from an entity that the registrant is no longer authorized by the entity to submit electronic documents on its behalf;

(5) Require that the registrant periodically renew his or her electronic signature agreement, under terms that the Administrator determines provide adequate assurance that the criteria of paragraphs (a) and (b) of this section are met, taking into account both applicable contractual provisions and industry standards for renewal or re-issuance of signature codes or devices.

(e) Electronic signature/certification scenario. An acceptable electronic document receiving system that may be used to accept electronic documents bearing an electronic signature must:

(1) Not allow an electronic signature to be affixed to the electronic document until:

(i) The signatory has been provided an opportunity to review all of the data to be transmitted in an on-screen visual format that clearly associates the descriptions or labeling of the information being requested with the signatory's response and which format is identical or nearly identical to the visual format in which a corresponding paper document would be submitted; and

(ii) The signatory takes affirmative action to affix his or her electronic signature~~A certification statement that is identical to that which would be required for a paper submission of the document appears on-screen in an easily-read format immediately above a prompt to affix the certifying signature, together with a prominently displayed warning that by affixing the signature the signatory is agreeing that he or she is the authorized signature holder—referred to by name—has protected the security of the signature as required by the electronic signature agreement signed under paragraph (d)(3) of this section and is otherwise using the signature in compliance with the electronic signature agreement~~;

(2) ~~Automatically r~~Respond to the receipt of an electronic document with transmission of an electronic acknowledgment in a timely fashion that:

(i) States that the signed electronic document has been received, clearly identifies the electronic document received, indicates how the signatory may view ~~and download~~ a copy of the electronic document received ~~from a read-only source~~, and states the date and time of receipt; and

~~(ii) Is sent to an address whose access is controlled by password, codes or other mechanisms that are different than the controls used to gain access to the system used to sign/certify and send the electronic document;~~

(3) Automatically creates an electronic ~~"copy of record"~~archive of the submitted report ~~that includes all the warnings, instructions and certification statements presented to the signatory during the signature/certification scenario as described under paragraph (e)(1) of this section, and~~ that:

(i) Can be viewed by the signatory, in its entirety, on-screen in a human-readable format that clearly and accurately associates all of the information provided by the signatory with the descriptions or labeling of the information that was requested;

(ii) Includes the date and time of receipt stated in the electronic acknowledgment required by paragraph (e)(2) of this section;

~~(iii)Has an agency electronic signature affixed that satisfies the requirements for electronic signature method under paragraphs (c) (3), (c) (4), and (c) (5) of this section;~~

(iv) Is archived by the system in compliance with requirements paragraph (g) of this section;

(v) Is made available to the submitter for viewing ~~and down loading~~ in a timely fashion; and
(vi) Is protected from a unauthorized access.

(f) Transaction Record. An acceptable electronic document receiving system must create a transaction record for each received electronic document that includes:
~~(1) The precise routing of the electronic report from the submitter's computer to the electronic document receiving system;~~
(2) The precise date and time (based on the system clock) of:
(i) Initial receipt of the electronic document;
(ii) Sending of electronic acknowledgment under paragraph (e)(2) of this section;
(iii) ~~Copy of record~~Archive created under paragraph (e)(3) of this section;
(3) ~~Copy of record~~Archive as specified under paragraph (e)(3) of this section.

(g) System archives. An acceptable electronic document receiving system must:
(1) Maintain:
(i) The transaction records specified under paragraph (f) of this section, and
~~(ii) Records of the system on-screen interface displayed to a user under paragraph (e) of this section that can be correlated to the submission of any particular report (including instructions, prompts, warnings, data formats and labels, as well as the sequencing and functioning of these elements);~~
(2) Maintain the records specified under paragraph (g)(1) of this section for at least the same length of time as would be required for a paper document that corresponds to the received electronic document, and in a way that:
(i) Can be demonstrated to have preserved them in their entirety without alteration since the time of their creation; and
(ii) Provides access to these records in a timely manner that meets the needs of their authorized users.

Sec. 3.3000 How are authorized State, tribal or local environmental programs modified to allow electronic recordkeeping?

(a) State, tribes, or local environmental programs that wish to allow the maintenance of electronic records or documents in satisfaction of requirements under such programs must revise or modify the EPA-approved State, tribal, or local environmental program to ensure that it meets the requirements of this part. The State, tribe, or local government must use existing State, tribal or local environmental program procedures in making these program revisions or modifications.
(b) In order for EPA to approve a program revision under paragraph (a) of this section the State, tribe, or local government must demonstrate that records maintained electronically under this program will satisfy the requirements under Sec. 3.100 of this part.

Sec. 3.4000 [Reserved]